METHOD AND APPARATUS FOR PROVIDING SPECIALIZED E-MAIL SERVICES OVER A COMMUNICATIONS NETWORK

BACKGROUND OF THE INVENTION

Field of the Invention.

This application generally relates to electronic mail (e-mail) communications, and, more specifically, to a method and apparatus for providing specialized e-mail services over a communications network, including providing to sender and/or recipient confirmation of delivery, opening of sent e-mails and/or verification of identity of sender and/or recipient.

Description of the Prior Art.

It is becoming increasingly difficult and/or impractical to do business without resorting to or relying on e-mail. Research shows that widespread use is making e-mail critical to corporations. It is estimated that the total number of e-mail boxes increased from approximately 198 million at the end of 1997 to 325 million at the end of 1998. In 1998, there were 77 million e-mail users in the United States sending 246 million e-mail messages a day. By 2002, it is estimated that this will escalate to 131 million users creating 576 million messages a day on the Internet.

Electronic messages (e-mails) are therefore becoming increasingly important and, also, increasingly accepted for sending important messages that have commercial and/or legal ramifications.

Many corporations, as well as medium- to small-sized businesses are conducting more and more of their business on the web. These businesses and individuals are seeking to move their communication as well as business transactions to the web for a variety of reasons. Many

see the web as a way of receiving data, contracts, etc., instantaneously rather than using the traditional overnight delivery companies. They also see the web as an alternative to expensive overnight package delivery and local courier services. It allows them to save money as well as increase the bottom line by not delaying the business decision-making process. Yet many companies are still hesitant about relying exclusively on e-mail because of the perception that "cyberspace" documents do not provide the same evidentiary safeguards that are available for postal or other delivery services. These companies are concerned about various issues, and are seeking a more secure and reliable alternative to traditional e-mail.

Just as with conventional notifications available with ordinary mail, it is frequently important to be able to verify or confirm that a message has been received by the intended recipient. Currently, e-mails are sent on both Intra- and Internet service providers (ISPs). While the sender is frequently provided with a message that the message "has been sent," such message is typically very temporary in nature and the sender does not have a reliable method of verifying, at a later date, that the message was sent. Equally important, the sender does not typically have any way of verifying or confirming that the intended recipient indeed opened the electronic mail and, therefore, has read it.

While it may be possible to print a copy of the screen indicating that a message "has been sent," this does not provide the reliability that the message was sent to a specific e-mail address or that, as noted, the intended recipient "opened" and, therefore, read the mail. A few Internet service providers (ISPs), such as AOL and Microsoft, do offer a limited service only to their own subscribers. This service allows the sender of an e-mail message using one ISP to receive a notification that the e-mail was opened by another subscriber using the same ISP. However,

there is currently no way of determining whether the message was opened and read, or simply opened, by the intended recipient, and there is no way of determining whether the message was opened by the intended recipient or by someone else having access to the e-mail account. Even this limited service is not currently available when e-mail messages cross between different ISPs.

Pitney Bowes, for example, has a product "*iSend.*" *ISend* tracks and verifies document delivery to sender via e-mail return receipt. The sender receives confirmation of the exact date and time the recipient retrieves the package. *ISend* seamlessly interfaces with all existing e-mail applications. *ISend* message recipients require no special software or proprietary protocols. Anyone with e-mail and web access can use it to send and receive deliveries.

UPS, through *UPS Document Exchange*, offers a product "*UPS Online Courier.*" *UPS Document Exchange Online Courier* also verifies receipt of electronic deliveries via e-mail. The sender has the option of requesting return receipt when shipping a document. An e-mail verifying receipt , if requested by the sender, is sent when the recipient accesses a document for a fee. Another feature of this product is its universal compatibility. Universal compatibility permits the sending and receiving of documents created in virtually any software.

E-mail outsourcing companies are also providing large corporations with secured e-mail services that provide such features as tracking and response. Critical Path, Inc., Mail.com, Inc., and Comm Touch Software, Ltd. are just a few of these e-mail outsourcing companies. Critical Path, Inc., provides business-to-business Internet message solutions for corporations, Internet service providers (ISPs), web hosting companies and web portals. In October 1999, Pitney Bowes began using Critical Path technology to bring the power of the *ISend* Online Document Delivery Service to the LAN e-mail desktop. Through this relationship, business users can

access *ISend* directly from within existing desktop e-mail clients – including MS Exchange, Outlook, Lotus Notes, Novell GroupWise, MS Mail, Lotus cc:Mail, POP3 and IMAP4 systems – to send secure, trackable messages.

It seems that every company that has ventured into the e-mail messaging world has had two major concerns: Security and Receipt Verification. Security is dealt with in different ways, and with various encryption methodologies by each company. However, e-mail receipts using alternative methods do not appear to have been explored. All companies that have entered the e-mail messaging arena offer tracking and return e-mail as the method in which verification is provided to the sender that the intended recipient has received his or her e-mail.

United Parcel Service has entered the e-mail messaging world via UPS Document Exchange and only provides tracking and receipt via electronic means. And yet, when its parent company, United Parcel Service of America, delivers any packages via its traditional ground and express courier methods, consumers are offered a variety of ways to ensure that their packages are received. The consumer has a variety of ways to track his or her package. Consumers either track by telephone or via the web, and a hard copy of the signature is provided via fax, through USPS or by printing same off the web. If the sender chooses to print the receipt via the web, obviously no charge is assessed. Yet if the sender requests a fax or a hard proof of delivery, an additional charge is assessed for each successfully transmitted or mailed P.O.D.

Even with these methods available, many traditional organizations, as well as individuals, use another option provided by UPS. At the time a shipper tenders a package to UPS, that shipper may request Delivery Confirmation Service by indicating Delivery Confirmation on the shipping record or by affixing a Delivery Confirmation label. Each Delivery Confirmation

response includes the date of delivery and either the name of the recipient or the disposition of the package. All responses are consolidated and provided to the shipper every week, in printed or electronic format. What makes this additional service interesting is that it is widely used by UPS's customers, even though the same information is available through the worldwide web.

Another crucial element of secured e-mail is not just to ensure that the secured e-mail has been received, but also to eliminate the "postcard" configuration of traditional e-mail, i.e., the fact that anyone along the way can read a given e-mail's content. If one is sending an electronic document that is highly sensitive or personal, it is crucial that only the intended recipient read it. Recent surveys of Internet users by groups like the Information Technology Association of America/Ernst & Young, L.L.P., Lycos and NetZero have consistently identified security and privacy fears as a top impediment to e-commerce.

Many techniques have been used in the attempt to ensure that only the selected recipient is able to read a particular piece of electronic mail. Some companies and examples are listed below:

- Tumbleweed Communications Corporation, through its Integrated Messaging Exchange Technology, offers a set of products and services that leverage the Internet and existing e-mail to enable secure, trackable and online communications. This corporation does so by posting the document on a server, safely inside the corporate network, and informing the recipient of the document's existence by e-mail. The recipient reads and retrieves the document using authentication and encryption technologies of protection. The server then confirms to the sender that the document was seen and received.

- Pitney Bowes, through its product *ISend*, guarantees that the intended recipient is the only one to view the e-mail through its use of leading edge security. *ISend* uses several layers of security, including up to 128-bit encryption, password protection, secured socket layer and recipient authentication. Once the document / package is sent, the file is quickly uploaded to a secure Pitney Bowes *ISend* server located in a Level 5 secure data center. There it is stored in a secured, encrypted format (using 128 bit RSA™ technology) while awaiting pickup. Once the package is delivered, the server assigns a randomly generated URL to the package with their existing e-mail and web browser software.
- British-based Software Company, through London's 1on1mail.com, has developed a system with military-style encryption that is so high; it would be illegal to export if the company were based in the United States. *1on1mail.com* is different from other systems in that other systems leave the unencrypted versions of a message in the memory of the recipient's computer and with the Internet service providers that handled the message. Any one of these unencrypted versions can be recovered by a competent technician, often years after they have been "deleted." Messages sent through the *1on1mail* system can be retracted without a trace.
- *UPS Document Exchange Online Courier* is also highly secure and trackable. Similar to other products, Document Exchange is secure through 128-bit encryption and password protection. Anyone can enter an incorrect e-mail, but with password protection, even if such an e-mail goes to the wrong recipient, this

recipient cannot open it. Companies like Kana, Mustang Software, Inc., and EGain Communications Corp. are trying to make businesses out of managing and disbursing this flow with software known as response systems. Kana develops software to monitor the e-mail flow and make sure responses are sent, if possible without involving a human.

UPS Document Exchange has message memory. UPS's server stores the content of sent messages in encrypted form on its server, along with delivery details. Transactional information is saved for one year. The contents may be saved on the UPS Online Courier server for up to thirty days.

As previously discussed, it appears that all providers of secured e-mail provide confirmation of receipt via an electronic means. An electronic e-mail is sent to the sender once the intended recipient receives the e-mail. Even traditional transportation companies such as UPS that have ventured into the document exchange market do not offer to their users of this service this alternative way of receiving confirmation, even though, for their more traditional products of physical package shipping, delivery confirmation is provided electronically as well via the USPS (through the more traditional Proof of Delivery or through another product offering known as "Delivery Confirmation").

As stated previously, only confirmation in electronic form is provided to senders of secure e-mails. An already noted example is *iSend* by Pitney Bowes, which functions as follows. First, the secure document is uploaded through secure connections by the sender to *iSend* server with optional recipient password. Second, the server notifies the recipient via e-mail and provides individual URL to retrieve the document. Third, the recipient enters optional

password and retrieves document through a secure connection. Fourth, *iSend* tracks and verifies document delivery to sender via e-mail return receipt. No other option is provided to ensure that the recipient received and read the e-mail.

Bolero.net is a company working on a global initiative to facilitate paperless international trade via the Internet. It offers many special features – open technical standards, supporting networks that use IP (the Internet Protocol), as well as having messages that are sent via the *bolero.net* system adhere to SMTP mail protocol. Yet, when it comes time to inform senders if the recipient received that crucial trade transaction or international legal document, it does so via e-mail. Again, no hard copy or any other verification of receipt is provided.

As stated previously, the offering provided by United Parcel Service through *UPS Document Exchange* provides only an electronic receipt for a fee. The service does allow the capability to audit the package trail. The sender can track and verify time of receipt, opening and printing, and length of time the recipient spent reading the package. The sender must request a return receipt.

As companies have ventured into the Internet's secured e-mail arena, many obstacles were found that were in the way of any kind of ease of use. For example, it was not possible for the sender to receive information concerning the package (e-mail) if the recipient was using a different Internet provider, or if sender and receiver had different software applications on their computers. Along with fears about e-mail security, these obstacles impeded the progress and expansion of e-mail as an alternative to overnight delivery couriers or USPS mail. The companies previously discussed quickly learned how necessary it would be to change the method in which they were to use e-mail, if at all.

UPS entered the electronic document market in 1998 with two product offerings, *UPS Online Courier* and *UPS Online Dossier.* In the beginning, *UPS Online Courier* offered a more secure version than traditional e-mail. The sender needed either to install software on his or her computer or to access it from the Internet. All the receiver needed was an e-mail address and Internet access. There was nothing provided in the way of high-level security or encryption. *UPS Online Dossier* was created for customers who needed the highest level of security. However, it required both sender and receiver to install software on their computers. In June1999, the new *UPS Document Exchange Online Courier 3.1.* had its debut. The *UPS Online Courier 3.1* version is compatible with standard desktop operating systems and offers full visibility real-time tracking, record retention, delivery confirmation and a password protection option. Further, no special software is required.

The company *Occams-razor.com* specializes in the electronic transfer of billing information. This eliminates the traditional barriers to electronic legal invoicing by differentiating and translating invoices sent in multiple formats. Using *Occams* product ShareDOC/LEGAL is easy as translating invoices sent in multiple formats, and as easy as e-mail. It requires nothing more than a browser and Internet access. The sender under this system is able to receive an electronic confirmation of receipt.

Pitney Bowes has joined forces with *SAPAG* to make web-based messaging easier, more reliable and more secure than ever before. Pitney Bowes' *iSend*™ Online Document Delivery System is now available via SAP.com ™ Marketplace; and, together, these services enable corporations to send and track the delivery of any file securely and reliably to anyone with an e-mail address on the Internet. It is the goal of companies entering this arena to have and provide an open collaborative

business environment. *ISend* recipients require no special software or proprietary protocols.

In some cases, as noted, electronic receipt information is available if companies /individuals are using different ISPs. The electronic receipt can sit at the application level such as with Tumbleweed or with UPS Document Exchange. None of the above-discussed companies, however, have ventured into providing senders with a proof of receipt that the document was received, or has been read, other than an electronic receipt. It is true that an audit trail is available marking where the document is, whether it was sent to an incorrect e-mail address, etc., and in many instances this tracking information is saved for up to 90 days – but, again, only in electronic format.

Most companies that offer this secure electronic messaging service do provide a service for what they have labeled "oops" e-mail. In many instances, an e-mail transaction can be blocked right up to the second before it is received and/or opened by the intended recipient.

In the overnight courier market, as well as in traditional ground delivery networks, carriers have provided information about a given package by means of a tracking number affixed to the package. The package is scanned and the data is available via the web and/or by calling the carrier. USPS and United Parcel Service offer additional alternatives for confirming or obtaining proof of delivery. Other carriers also provide additional ways of obtaining proof of delivery, but are more limited when compared to the U.S. Post Office or UPS.

The USPS has another service, "USPS Merchandise Return Receipt." This is available for all USPS services. There is an additional charge for each merchandise receipt requested. In order to use this service, shippers must attach a completed return receipt form to the package. After the package has been delivered, the receipt – including consignee signature and date delivered – is mailed back to the sender.

United Parcel Service has another service for verifying that a package has been delivered – "Delivery Confirmation," which was discussed above. Customers who select this additional service must do so at the time of shipping. Shippers who request Delivery Confirmation receive a printed response from UPS by mail, confirming the delivery. Responses are also available in electronic format (magnetic tape or EDI).

These services are provided and used by customers even though the physical packages are tracked and delivery information is available and can be printed from the worldwide web.

It appears that customers who select this additional service are trying to obtain additional confirmation in the form of written proof in order to ensure delivery of high-value shipments, comply with government regulations and to facilitate payment collection. To what degree USPS Merchandise Return Receipt or UPS Delivery Confirmation is at present used has not been disclosed. Yet even though tracking has been available via the web for quite some time, neither carriers nor their competitor RPS have chosen to delete this option from their service offerings. Although in the traditional world of package and document delivery there are many ways of receiving tracking information as well as delivery receipt confirmation, in the secure e-mail world only electronic means are available. All the electronic services state that their systems are secured, yet not one provides a 100% guarantee that the secured e-mail was actually received by the intended recipient.

For example, all highly secured e-mail programs provide the highest security through encryption and a password. Yet the password, in one way or another, must be communicated with the recipient. UPS Online Courier allows the sender to use either the Online Courier account password or a unique password that the sender can create. But how does one prevent the password falling into the wrong hands?

In order to make senders more confident about exploring a more extensive use of secured e-mail, perhaps an additional or alternative delivery confirmation receipt should be explored.

The USPS offers consumers a variety of methods to receive confirmation or receipt of delivery for traditional packages and documents. However, there are exceptions depending on the type of package and its destination.

- Certificate of Mailing is a receipt showing evidence of mailing. It can be purchased only at the time of mailing. The certificate does not provide insurance coverage for loss or damage, nor does it provide proof of delivery. No record is kept at the mailing office, and a receipt is not obtained when mail is delivered to the addressee.
- Certified Mail provides proof of mailing and of delivery of mail. The sender receives a mailing receipt at the time of mailing, and a record of delivery is kept at the recipient's post office. A return receipt providing the sender with proof of delivery can also be purchased for an additional fee. Certified mail service is available only for first class mail or priority mail. Certified mail is not available for international mail. And Certified Mail does not offer insurance protection. For valuables and irreplaceable items, Express Mail or insured or registered mail must be used.
- Registered Mail is the most secure option offered by the U.S. Postal Service. It provides added protection for valuable and important mail. Registered articles are placed under tight security from the point of mailing to the point of delivery. First class mail or priority mail postage is required on domestic registered mail. Return receipt and restricted delivery services are available for additional fees, and insurance can be purchased on domestic registered mail at the sender's option.

- Return Receipt is the sender's proof of delivery. A return receipt can be purchased for mail sent cash-on-delivery (COD), Express Mail, mail insured for more than $50.00, registered mail or certified mail. The return receipt shows who signed for the item and the date that it was delivered. Unless prohibited by law, the return receipt also provides the delivery address if the address on the piece of mail is no longer correct. Return receipt service can be purchased in conjunction with restricted delivery service. It can also be requested before or after mailing, except for return receipt for merchandise service.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to provide a method of providing specialized e-mail services which eliminates the disadvantages inherent in prior art methods.

It is another option of the present invention to provide a method of providing specialized e-mail services which is simple to implement and use.

It is still another object of the present invention to provide a method of providing specialized e-mail services as in the previous objects which is reliable and provides safeguards to commercial and/or legal rights as between the parties communicating by e-mail.

It is yet another object of the invention to provide a method of providing specialized e-mail services which include the ability to provide notification to a sender that an e-mail has not only been sent but also opened and, therefore, presumably read by an intended recipient.

It is a further object of the invention to provide a method of providing specialized e-mail services to a sender, a recipient or both.

It is still a further object of the invention to provide a method of providing specialized e-mail services which allows the sender to request identification verification before the sending computer is authorized to send an e-mail, as well as identification verification of a recipient before the recipient is allowed to open an e-mail.

It is yet a further object of the invention to provide a method of providing specialized e-mail services which allows a recipient of an e-mail to request identification verification of a sender prior to opening received e-mail.

It is an additional object of the invention to provide a method of providing specialized e-mail services which provides safeguards to recipients of e-mails against viruses that can be harmful to recipient's computer system.

It is still an additional object of the invention to provide specialized e-mail services which allow the sender of the e-mail to request that the notifications received by the sender that e-mail has been opened can be stored for a pre-determined period of time for future possible use and reference.

It is yet an additional object of the invention to provide a method of providing specialized e-mail services which allows both the sender and the recipient to request that the contents of the e-mail message be stored for a pre-determined period of time for future possible use and reference.

It is also an additional object to provide a notification and registration system and method of confirming delivery of electronic message on Intra- and Internet providers that simulate a wide range of products, services and protections to both the sender and the recipient.

It is also another object of the present invention to provide a method providing

specialized e-mail services which makes it possible to obtain notification and verification of the type aforementioned, which can be implemented between subscribers of the same Internet Service Providers (ISPs) or subscribers to different ISPs.

In order to achieve the above objects, as well as others which will become evident hereinafter, a method providing specialized e-mail services to a sender, recipient or both over a communications network includes the steps of establishing an online session on a computer operated by an e-mail sender with a computer at an e-mail center, and sending, by the sender, an e-mail packet including an e-mail message destined to a recipient together with a request for a specified verification e-mail service to the e-mail center. The e-mail center computer transmits the e-mail to an e-mail address accessible by a computer operated by an intended recipient. Same e-mail center receives notification when said recipient at least receives and opens said e-mail and, providing, by the e-mail center, at least requested e-mail notification to said center.

Specialized services to be provided to sender, recipient or both include notification that e-mail was opened, notification that e-mail was opened by intended recipient, notification of time and/or date of opening of e-mail, storage for future access of any selected notification information, storage of e-mail message content for future access, as well as verification of identity of sender and/or recipient. Other notifications and/or verifications are possible and may be used in conjunction with the invention. For example, the sender may want to obtain notification as to the e-mail services requested by the recipient (e.g., storage of document text, verification of identity, etc.).

BRIEF DESCRIPTION OF THE DRAWINGS

With the above and additional objects and advantages in view, as will hereinafter appear, this invention comprises the devices, combinations and arrangements of parts hereinafter described by way of example and illustrated in the accompanying drawings of preferred embodiments in which:

Fig. 1 is a schematic block diagram illustrating the system for providing specialized e-mail services to a sender, recipient or both in accordance with the present invention;

Fig. 2 is a flow chart illustrating one presently preferred sequence of method steps for implementing the method in accordance with the invention and illustrating three special services that may be requested, it being understood that other specialized e-mail services may also be included;

Fig. 3a is a flow chart illustrating the details of the method illustrated in Fig. 2 as it relates to the request of a return receipt by a sender without identification verification;

Fig. 3b is a flow chart illustrating the details of the method illustrated in Fig. 2 as it relates to the request of a return receipt by a sender with identification verification;

Fig. 4a is a flow chart illustrating the details of the method illustrated in Fig. 2 as it relates to the request of certification by a sender without identification verification;

Fig. 4b is a flow chart illustrating the details of the method illustrated in Fig. 2 as it relates to the request of a certification receipt by a sender with identification verification;

Fig. 5a is a flow chart illustrating the details of the method illustrated in Fig. 2 as it relates to the request of a registration by a sender without identification verification;

Fig. 5b is a flow chart illustrating the details of the method illustrated in Fig. 2 as it

relates to the request of a registration with identification verification.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now specifically to the Figures, in which similar or identical parts are designated by the same reference numerals throughout, and first referring to Fig. 1, a system for providing specialized e-mail services in accordance with the invention is generally designated by the reference numeral 10.

The system 10 and method of providing specialized e-mail services in accordance with the invention can be used to provide such services to a sender, recipient or both over a communications network. In Fig. 1, an e-mail sending computer used by the sender of an e-mail message is designated by the reference numeral 12. In accordance with a preferred embodiment of the invention, the computer 12 has associated therewith a sender identification verification unit 14 linked to the computer 12 by means of a suitable link or line connection 16. The sender verification unit 14 may also be built in or incorporated into the computer 12 itself. The specific manner in which the verification unit 14 cooperates with the computer 12 is not critical, and any identification verification unit may be used. From the field of biometrics it is known that it is possible to verify the identity of a user in numerous ways, including checking the user's fingerprints, retinal identifying information, voice patterns, etc. These and other biometric approaches may be used in connection with this invention for both the sender as well as the recipient, as will be described hereafter.

The computer 12 is connected in any conventional way by means of a link 18 to a communications network. In the presently preferred embodiment, such communications network

is shown as the Internet 20. However, it will also be evident that this invention can be used also in connection with other communications networks, include private, quasi-public and public networks. These include local, Intranet and dial-up networks.

In a typical situation, the user of the sending computer 12 needs to electronically transmit an e-mail message, document or attachment to an e-mail to a specific recipient, represented by receiving computer 22. In the conventional manner, the sender uses any traditional or available e-mail software and composes a message and/or attaches to his or her message any suitable document. The sender then transmits the contents of the e-mail message, together with any attachments, to the recipient's e-mail address. Such conventional method of sending an e-mail directly to a recipient is represented by the dash line 24. Of course, the connection shown is not precise, and the representation is merely illustrative to facilitate the discussion. Depending on the Internet Service Provider (ISP) used by the sender, and depending on the ISP used by the recipient, the e-mail message may be routed to various servers until the message is lodged on the server of the recipient's Internet provider. The intended recipient, in turn, can access his or her ISP's server and retrieve his or her message. As suggested in the "Background of the Invention," once the sender's e-mail is forwarded and finds its way the recipient's e-mail server, the sender is provided with a message that the message has been "sent." The recipient is typically provided with a message that there is "new mail." The recipient can, if he or she desires, open such new mail. Otherwise, such new mail can be ignored or deleted. The sender does not typically know what the fate of his or her message is, and whether such message is, in fact, ever read by the recipient. With some ISPs, subscribers of the same ISP can, in some instances, be notified that their messages have actually been opened. Such service is provided by AOL and MSN.

However, currently, such limited service is not provided across different ISPs.

An important feature of the present invention is that the sender or user of the sending computer 12 has certain options, as does the intended recipient. Thus, the sender can request specialized e-mail services, and the recipient can likewise be provided with certain options prior to or subsequent to opening the mail received from the sender. However, in order to provide some of these additional e-mail services, it may be necessary or desirable to provide a receiver verification unit 26 associated with the computer 22 in any suitable or conventional way. The verification unit 26 may, as with the verification unit 14, also be built in or incorporated into the receiving computer 22 itself. Again, the specific manner in which the verification unit 26 cooperates with the computer 22 is not critical, and any identification verification unit may be used to identify the identity of the recipient. Any biometric device suitable for the purpose may be used and may be the same as or different from the biometric device used to verify the identity of the sender 14.

In order to achieve the objectives, advantages and/or benefits of the present method, an important feature of the invention is the provision of an e-mail center 30 which is in the form of a server linked by any suitable means, at 32, to the Internet 20. An important feature of the invention is that a message to be sent by the sending computer 12 to the receiving computer 22 is no longer a "direct" transmission represented by the dash line 24, but such message is first transmitted to the e-mail center 30 by means of a path 34. The transmission of the message represented by the dash line 34 is achieved by having the sending computer 12 establish an online session with the computer and e-mail center 30. Now, instead of the sender sending only a message to an intended recipient, the sender sends an e-mail packet via path 34 which includes

both the e-mail message destined to the recipient, together with any attachment and a request for specified special e-mail service(s) to the e-mail center 30. The e-mail center 30, in turn, transmits the sender's e-mail message to an e-mail address accessible by a computer operated by the recipient, by way of path 39. In the normal course, a simple re-transmission of the message by the e-mail center 30 to the intended recipient would have all of the characteristics of the original e-mail had it been sent directly by the sending computer 12 to the receiving computer 22 by way of direct path 24. However, in order to provide the greatest spectrum of e-mail services, the work station representing the receiving computer 22 and/or the ISP of the recipient is advantageously provided with software that can ascertain if and when the intended recipient actually opens the e-mail message. Such software, at the receiving end, makes it possible for the e-mail center to receive notification as to when the recipient at least receives the e-mail and, as noted, as to when the recipient opens such e-mail. Such notification to the e-mail center 30 may also be represented by the dash line 39 as a path of data transmission between the receiving computer 22 and the e-mail center 30. Once such notification is received by the e-mail center, an important feature of the invention is the re-transmission of at least part of or all of the information received by the e-mail center back to the sender, as may have been requested or contracted by the sender. Thus, the more services that the sender requests and contracts to receive, the more such information may be transmitted to the sender under any given circumstances.

Preferably, the sender establishes a secure session with the e-mail center 30. While it is preferable that the communications between the sender, recipient and the e-mail center be as secure as possible, the primary feature or essence of the present invention is not strictly security

to prevent authorized people from having access to messages but the ability to establish evidence that certain information was transmitted to a person who has received and read such information. At one level, therefore, the essence of the present invention is to provide special mailing services somewhat analogous to the specialized services provided by the U.S. Postal Service in the form of return receipt requested, certified mail and registered mail.

The broadest aspects of the method in accordance with the present invention, and associated system hardware, will be generally described in connection with Fig. 2. The computer desktop 40 generally corresponds to the sending computer 12 shown in Fig. 1. Initially, the sender is required to log on to the e-mail center 30. However, as indicated, such log-on may take place through the Internet, direct dial, etc. In the discussion that follows, the communications network will be assumed to be the Internet, those skilled in the art being fully aware of the changes or modifications that would need to be made to access the e-mail center 30 by means of another, alternative communications network. Thus, at 42, the user/sender logs on to the Internet in a conventional manner, such as by dial-up, direct 56 k-line, DSL, T1, etc. Preferably, any attempt to log on to the mail server will prompt the user, at least initially, to indicate whether the desktop is provided with the e-mail center software on the user's machine at 46. If such software does not exist, the computer is set up to launch a browser and access the e-mail center web site. Responding in the negative launches the user's browser, at 48, to access the e-mail center web site, the software of the e-mail center being downloaded to the user/sender at 50. Once such software is downloaded, the user can install such software on the station or desktop, at 52. This can place a short cut icon on the user/sender's desktop for activating the e-mail center software.

In order to initiate a transmission of an e-mail to an intended recipient, with request for

additional e-mail services, the sender can click on the icon on the desktop, at 54, to activate the e-mail center software. Such software queries the sender as to whether to access the e-mail center. If the sender selects "NO," the sender can work off-line and, for example, compose mail off-line, at 58. After such mail has been composed, the e-mail center software can again query as to whether the sender wishes to access the e-mail center to send such composed mail. At 60, the sender is again prompted as to whether the e-mail center is to be accessed so that the mail composed at 58 can be sent. If the answer is "NO," the sender may be prompted as to whether such mail is to be saved, at 62. In the event the user wishes to access the e-mail center, either at 56 or at 60, the user can activate the default browser at 64 to access the home site of the e-mail center, which would provide the sender with a series of options. Once at the e-mail center home page, the sender can, at 66, activate a desired web services page for sending a message to the intended recipient. In the event that the user has not composed mail "off-line," the sender may, after opening sender's "Inbox" at 68, compose mail online, at 70.

It will be appreciated that the sequence of steps aforementioned is not critical, and certain of the steps may be transposed or interchanged. Thus, for example, the user may be prompted by the e-mail center software at 42 whether the user wishes to compose mail off-line. Clearly, the specific point at which the mail is composed is not important, as long as the user has an opportunity to compose the mail either off-line or online at some point prior to completing the session with the e-mail center.

Once the mail has been composed and is ready to be sent to the intended recipient, the e-mail center provides the sender with a series of options for special e-mail services. Such services fall into three primary categories. One group of services involves notification, the second is

storage of information and the third is identity verification. Notifications may include, but are not limited to, notification that an e-mail was sent, notification that an e-mail was received, notification that an e-mail was opened, notification that an e-mail was opened by the intended recipient, notification of time and/or date of receipt and/or opening of e-mail. Another e-mail service includes storage of any of the aforementioned notifications for future access and/or use. A further storage function is the storage of the actual e-mail message contents for future access and/or use. Finally, the e-mail center can provide verification of the identity of the sender and verification of the identity of the recipient to prevent unauthorized opening of an e-mail message that may be delicate in content, confidential and/or privileged.

At 72, the sender can make the selections of special e-mail services, this being exemplified at 74, 76 and 78, at which the sender can request "return receipt" at 74, that the e-mail message be "e-certified" at 76 and/or that the e-mail message be "e-registered" at 78. These illustrative services can be briefly explained as follows. When the sender requests a "return receipt," at 74, the e-mail center is being requested to provide the sender with a notification that the e-mail was sent, received and/or was opened by a recipient operating the e-mail receiving computer 22. This is to be distinguished from verification of identity of recipient, as will be discussed hereinafter. The second option, at 76, is "e-certification" of mail, which involves the storage of the requested notification in the e-mail center data storage bank 36. The third option, at 78, is similar to the previous options, with the exception that in addition to storing the notification and/or verification information regarding the identity of the recipient, the e-mail center 30 additionally stores the contents of the e-mail in the data storage bank 36 for future access and/or use.

As will be noted from Figs. 2-5b, the procedures or sequences of steps for all three options are substantially similar or the same, with the exception of what is stored or not stored for future use. These differences aside, the method steps, procedures or functions are generally the same for all three options and, therefore, only Figs. 3a and 3b will be discussed in detail, such discussion also being applicable to Figs. 4a, 4b, as well as Figs. 5a, 5b, with the only exceptions having been noted, and to be indicated again below.

To initiate a "return receipt" by the sender without the request for verification of identity of recipient, reference is made to Fig. 3a, in which the sender chooses to send the composed e-mail at 86, and such mail is routed to the e-mail center 30 by way of path 34, as aforementioned. At 90, the e-mail center routes the mail to the intended recipient, by way of path 39. The e-mail center then tries to establish whether the intended recipient has the e-mail center software on the recipient's work station or receiving computer 22. This check can be conducted either prior to or subsequent to the routing of the mail to the recipient at 90. Such determination can be made from information stored in the data storage bank 36 of the e-mail center. Thus, if the e-mail center had shipped such software to the intended recipient and/or the intended recipient had previously registered or used the service, such information would be available to the e-mail center. If the e-mail center 30 determines that the intended recipient does not have the required software, the recipient or user may be prompted to download the software, at 94, such as by sending a separate e-mail message by the e-mail center 30 to the intended recipient. The reference numeral 96 represents a successful download by the intended recipient of the software.

If the recipient has the requisite e-mail center software, or has successfully downloaded such software, at 96, the intended recipient can then open the e-mail message, at 98. As soon as

such e-mail is opened by the intended recipient, a hidden back-end action or auto-response is initiated by the e-mail center software on the recipient's work station, at 100, which is in the nature of a hidden action, or transparent to the recipient. However, once such auto-response has been generated, the "action" taken transmitted to the e-mail center at 102. Receipt of such information by the e-mail center of such information enables the e-mail center to route a "return receipt" back to the original sender, via path 34, to confirm and notify the sender of the outcome of the special services that have been requested. Once the return receipt has been forwarded to the sender's e-mail address, the sender can print out such return receipt for future reference and use. Such would normally terminate that transaction.

In Fig. 3b, which is generally similar to Fig. 3a, with the exception that a sequence is illustrated that may be used to provide verification of identity of the recipient should such special service have been requested by the sender. Thus, at 106, the sender is prompted as to whether the sender wishes to verify the identities of both the sender and the recipient. In some instances, the sender may set up a default to also require verification of the sender to ensure that e-mails cannot be transmitted from his or her "Inbox" by an authorized party. If the sender wishes to verify both the sender and the recipient, the sender can verify his or her own identity at 110 by using the sender verification unit 14. As indicated, such verification unit may take any suitable form, and may use a biometric device associated with a computer. The verification units can, for example, read the individual's fingerprints, voice, anatomical features, retinal information, or the like. If such verification fails, at 112, the sender is prompted of such failure of verification, at 114, and the e-mail center software may be set up to default in those circumstances and block the sending computer 12 from sending any messages from either such computer or any other

computer using the sender's "Inbox." However, if the sender does not require that his or her identity be verified, the e-mail center software can be requested to only verify the identity of the recipient, at 108. The recipient verification step, at 108, is implemented at the recipient's work station 22.

If sender verification is successful, the sender can choose to send composed mail, at 86, and route the mail from the sending computer 12 to the e-mail center 30, at 88. Such mail can then be routed to the recipient, at 90. As indicated previously, the e-mail center 30 can try to establish whether the intended recipient already has the e-mail center software on the desktop or receiving computer 22, at 92. Such determination can be made either by sending a separate e-mail to the intended recipient, prior registration by the recipient, prior mailing of the software to the recipient or the like. Again, if it is established, at 92, that the intended user or recipient does not have the e-mail center software, at 92, the user or recipient may be prompted to download such software at 94. Any one of a number of conventional methods of prompting the recipient can be used. Once such software has been successfully downloaded, at 96, the user is prompted for verification using a biometric digital reader, at 116. This is a phase of the activity that differs from the services requested and exemplified in Fig. 3a. If the sender has requested verification of identity of the recipient, such verification may be performed by using the receiver verification unit 26. Of course, if the intended recipient does not have the benefit of or access to a receiver verification unit, such verification cannot be performed. Instead, the user can be prompted to obtain such receiver verification unit either by the e-mail center or from another suitable source.

If the verification fails, at 118, the sender is again prompted of such failure, and the intended recipient is not provided with the mail in a form that can be opened. However, if

verification is successful, the e-mail message is provided to the intended recipient, who can then open such mail. As previously noted, as soon as such mail is opened, a hidden back-end action in the form of an auto-response is sent back to the e-mail center 30, at 100. Such auto-response initiates the generation of an "action" confirmation through the e-mail center, at 102, and a return receipt is sent back to the original sender, at 104. Again, the sender can print out or store such return receipt for future access and use.

Referring to Figs. 4a and 4b, these are identical to Figs. 3a and 3b, respectively, as aforementioned. However, in both Figs. 4a and 4b, an additional "certification" step or function is provided in the sequence, designated by the reference numeral 120, at which the "certified" return receipt is stored in the data bank 36. Except for such storage for future reference and use, all of the other steps may be the same, with or without verification of identity. Similarly, in Figs. 5a and 5b, which are also generally similar to Figs. 3a and 3b, respectively, these represent additional protections for the sender. Not only can the sender store the "certified" return receipt, at 120, but also the e-mail contents in the data storage bank 36 of the e-mail center, at 122. Clearly, this provides additional safeguards in the event of a possible dispute between the sender and the recipient, as to what was sent by the sender, whether such information was read by the recipient, as well as the specific contents of the message that was read. There can be little or no dispute, accordingly, at least as to these issues, which are all documented in the data storage bank 36. This added feature is referred to as "registration" and a registered receipt is stored and routed to the sender, at 120 and 104 in Figs. 5a and 5b.

An important feature of the invention is also the ability of both the sender and the recipient to request and obtain specialized e-mail services. This is unlike the analogous services

provided by the U.S. Postal Service or other mail services, all of which are typically requested by and provided to the sender of a letter or package. Because of the structure and flexibility of computers and e-mail messengering in general, both the sender and the recipient can request, from their desktop, that they be provided with any of the aforementioned notifications for their own records, as well as a copy of the contents of the message sent and stored in the data bank.

Additionally, a feature of the present invention is that the intended recipient can, as a condition of opening a specified e-mail, first request verification identification of the sender. This may be helpful to a recipient in positively identifying that a certain communication was, in fact, transmitted by a specified individual. Furthermore, a e-mail recipient may also want to obtain position verification that an e-mail has, in actuality, been sent by a specified individual whose identity has been verified prior to opening an e-mail or attachment thereto. This may become increasingly important with the advanced viruses that proliferate in connection with e-mails and become more sophisticated and more difficult to monitor and detect. This is particularly true with many of the more contemporary viruses, which are programmed to indicate that a specified message has been sent to an individual from someone known to the recipient and with whom prior e-mail messages and possibly business has been exchanged. Viruses can, in many instances, masquerade themselves and cleverly select subject lines and specify other familiar information readily available from the recipient's or sender's computers to make it appear that it is a message or attachment that is safe to open. However, if such message or attachment was automatically sent by a virus, without the knowledge of the apparent sender, the recipient may very well want to positively verify that the sender intentionally forwarded or transmitted the message before the recipient opens the message. Therefore, unlike heretofore

known postal and other services provided to senders of information and products, the sender and recipient are now placed on a more even footing, as they should rightfully be, if such specialized e-mail services can become important from a legal or financial standpoint. Both parties to the transaction should, therefore, have the right and the opportunity to equally protect themselves and, thereby, hopefully try to avoid difficulty or conflicts in the future that might, in some instances, arise without such specialized e-mail services and their inherent positive evidentiary value and certainly.

An apparatus or system for achieving the objects of the present invention includes the elements, components or features illustrated in Fig. 1 for performing the functions or operations heretofore described.

Once set up, the e-mail center 30 is also an ideal vehicle for providing enhancements to e-mail services. For example, a sender can select greeting cards, wedding invitations and invitations for other celebrated occasions, mailers, business letters with concomitant letterhead and logo, and any other stationery or postal functions. A variety of web sites are available that provide some of the services mentioned.

The e-mail center 30 can, thus, provide visitors to the site with the ability to send free electronic greeting cards. Aside from free electronic greeting cards, this site can provide other services, for a fee. A visitor to this site can order physical (hard-copy) greeting cards for all occasions, wedding invitations, as well as balloons, baskets, stuffed animals, etc. The e-mail center 30 can also snail-mail physical (hard-copy) cards for the visitor. All the visitor needs to do is personalize the card. The e-mail center 30 can also offer other services such as stationery, supplies and business cards. It can offer an entire range of such services, or specialize in niche

services. The e-mail center 30 can also provide consumers with service contracts and preventive maintenance contracts. Customers that visit the site can order a variety of supplies such as New/OEM Cartridges and Facsimile Cartridges and supplies.

The e-mail center 30 may also be set up to provide e-mail based scheduling services. It can allow users to set up meetings and convey additional information, such as a meeting's address or participants. The e-mail center 30 can do so across the Internet, and not just within a corporate network, where Microsoft Outlook provides a similar function. Participants can reply by e-mail, and the e-mail center 30 can consolidate responses to determine when mutual .availability exists.

As noted previously, the present invention has been described in general terms, it being understood that the specific details or sequences of operations are not critical for the practicing of the invention. It will be evident to those skilled in the art as to what changes would need to be made in order to modify the described system hardware and/or software to achieve the same or other objectives of the invention.

While this invention has been described in detail with particular reference to preferred embodiments thereof, it will be understood that variations and modifications will be effected within the spirit and scope of the invention as described herein and as defined in the appended claims